10/709268

20

First Hit Previous Doc Next Doc Go to Doc#

□ Generate Collection Print

L7: Entry 1 of 3 File: PGPB Jan 6, 2005

PGPUB-DOCUMENT-NUMBER: 20050001711
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20050001711 A1

TITLE: System, method and apparatus for electronic ticketing

PUBLICATION-DATE: January 6, 2005

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Doughty, Ralph O.	Colleyville	TX	US	
Antaki, Patrick R.	Plano	TX	US	
Palmer, Glennard D.	Richardson	TX	US	
Gilliom, Robert M.	Wooser	AR	US	

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	COUNTRY	TYPE CODE
Innovation Connection Corporation	Richardson	TX		02

APPL-NO: 10/ 737080 [PALM]
DATE FILED: December 16, 2003

RELATED-US-APPL-DATA:
Application 10/737080 is a continuation-in-part-of US application 09/707559, filed November 6, 2000, ABANDONED
Application 10/737080 is a continuation-in-part-of US application 10/680050, filed October 7, 2003, PENDING
Application 10/680050 is a continuation-in-part-of US application 10/400306, filed March 27, 2003, PENDING
Application is a non-provisional-of-provisional application 60/368363, filed March 28, 2002,

INT-CL: [07] H04 Q 1/00

US-CL-PUBLISHED: 340/005.74; 340/005.82
US-CL-CURRENT: 340/5.74; 340/5.82

REPRESENTATIVE-FIGURES: 10

ABSTRACT:

The present invention provides a system, method and apparatus for securely granting access to an event. For example, in one embodiment of the present invention, an apparatus, such as an electronic card, ticket or information carrier, contains

biometric data about a user. When the "ticket" is purchased or authenticated, event access information is stored on the electronic card or ticket by an entity authorized by the event provider. The user is allowed access to the event when the biometric data stored on the electronic card or ticket matches the user's biometric data and the event access information is validated. The user's biometric data is authenticated via a biometric sensor on the electronic card or ticket. The user's biometric data can also be authenticated by the entity granting access to the event.

PRIORITY CLAIM

[0001] This patent application is a continuation-in-part of: (1) U.S. patent application Ser. No. 09/707,559 filed on Nov. 6, 2000; and (2) U.S. patent application Ser. No. 10/680,050 filed on Oct. 7, 2003, which is a continuation-in-part of U.S. patent application Ser. No. 10/400,306 filed on Mar. 27, 2003, which is a non-provisional patent application of U.S. provisional patent application Ser. No. 60/368,363 filed on Mar. 28, 2002.

Previous Doc Next Doc Go to Doc#

First Hit Previous Doc Next Doc Go to Doc#

□ Generate Collection Print

20

L7: Entry 1 of 3 File: PGPB Jan 6, 2005

DOCUMENT-IDENTIFIER: US 20050001711 A1
TITLE: System, method and apparatus for electronic ticketing

Abstract Paragraph:
The present invention provides a system, method and apparatus for securely granting access to an event. For example, in one embodiment of the present invention, an apparatus, such as an electronic card, ticket or information carrier, contains biometric data about a user. When the "ticket" is purchased or authenticated, event access information is stored on the electronic card or ticket by an entity authorized by the event provider. The user is allowed access to the event when the biometric data stored on the electronic card or ticket matches the user's biometric data and the event access information is validated. The user's biometric data is authenticated via a biometric sensor on the electronic card or ticket. The user's biometric data can also be authenticated by the entity granting access to the event.

Application Filing Date:
20031216

Summary of Invention Paragraph:
[0004] One way to increase the security of information bearing cards is the use of smart cards, also referred to as chip cards. Although smart cards 200 may also include a magnetic stripe, they primarily rely on an integrated circuit, also commonly referred to as a controller or processor, embedded within the plastic or laminated substrate 204 below the terminals 202 to store the cardholder's informatio~~n as shown in FIG~~. 2. The integrated circuit is communicably coupled to a set of metallic terminals 202 that are designed to interface with a special reader. Other common features of smart cards 200 that are well known to those skilled in the art, such as the cardholder's name, account number, expiration date, issuer, signature stripe, validation code, photograph, etc., are not shown. A smart card 200 is capable of incorporating multiple applications or accounts on a single card or other media. As a result, smart cards 200 are widely recognized as a viable way to improve the effectiveness and security of a given card or device. Such smart cards 200 require a different reader from the standard magnetic stripe readers that currently make up virtually the entire card reader infrastructure throughout the world. As a result, the acceptance and wide-spread use of "true" smart cards (without a magnetic stripe) has been slow.

Summary of Invention Paragraph:
[0007] Magnetic stripe cards, smart cards and wireless cards can be used to provide access to an event, such as a vehicle (e.g., airplane, train, bus, ship, etc.), a restricted area, a club, a concert, an entertainment venue or a sporting event, etc. With the rapid proliferation of computers and the Internet, the use of electronic ticketing has become very popular for both consumers and the ticket providers. Present electronic ticketing systems, however, require identification of the purchaser by presentation of some type of photo identification ("ID") issued by a government agency. The use of photo ID is not only a nuisance to the consumer, but also a potential security risk. For example, a customer's photo ID can be verified and an airline boarding pass properly issued. ~~Because the custome~~r's ID

may not be closely checked as the customer boards the plane, the boarding pass can be used by anyone. Thus, the airline security procedures can be bypassed in some cases.

Summary of Invention Paragraph:
[0010] To remedy the deficiencies of existing systems and methods, the present invention provides a system, method and apparatus for securely granting access to an event. For example, in one embodiment of the present invention, an apparatus, such as an electronic card, ticket or information carrier, contains validated biometric data about a user. When the "ticket" is purchased or authenticated, event access information is stored on the electronic card or ticket by an entity authorized by the event provider. The user is allowed access to the event when the biometric data stored on the electronic card or ticket matches the user's biometric data and the event access information is validated. The user's biometric data is authenticated via a biometric sensor on the electronic card or ticket. The ~~user's~~ biometric data ~~can also be~~ ~~authenticat~~ed by the entity granting access to the event.

Summary of Invention Paragraph:
[0012] The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the ~~use of o~~n-card/device biometric authentication of the user and pro~~grammable~~ magnetic stripes such tha~~t the data~~ within the tracks of the stripe can be spatially manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into the card or device. Alternatively, the data can be stored in the on-card processor/controller and then transmitted via time-varying signal to the card reader thereby emulating the swipe of a magnetic stripe through the magnetic card reader. In addition, the card or device can provide such information via a contactless communication system. These capabilities also enable multiple sets of data and applications to be incorporated onto a single card, device or media, thereby making it a universal card/device with numerous sets of data (e.g., accounts) and/or applications that can be temporarily downloaded onto the magnetic stripe from the memory of the on-card processor, used in the desired application, and then modified or erased. Finally, some or all of the above features can be disabled until the owner of the card enables them through use of an on-card biometrics sensor and logic that is pre-registered to the cardholder. As a result, maximum security is guaranteed since the card cannot be used if it is lost or stolen, and skimming can be virtually eliminated by prompt modification or erasure of the magnetic stripe data following the basic transaction authorized by the owner.

Summary of Invention Paragraph:
[0013] More specifically, the present invention provides an apparatus or user device that includes a substrate, a communications interface disposed within the substrate, a biometric sensor mounted on the substrate, a memory disposed within the substrate, event access information stored in the memory and a processor disposed within the substrate that is communicably coupled to the communications interface, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and transmit the event access information and an indication that the user is authorized to use the apparatus via the communications interface when the user is verified. A power source is also disposed within the substrate and electrically connected to the communications interface, the biometric sensor and the processor. The communications interface may include a wireless transceiver, an optical transmitter, a magnetic stripe, a programmable magnetic stripe or magnetic field generator that is normally inactive, a smart card interface or communications port. The magnetic field generator can create a spatial magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic

stripe card through a magnetic card reader.

Summary of Invention Paragraph:
[0014] The present invention also provides a method for requesting access to an event by a user of an apparatus containing a communications interface, a biometric sensor, a memory and a processor. The method includes the steps of receiving event access information from an external source via the communications interface and storing the access information in the memory, receiving authentication data from the biometric sensor, determining whether the authentication data is valid for the user, and requesting access to the event by transmitting the event access information and an indication that the user is authorized to use the apparatus via the communications interface whenever the authentication data is valid. Depending on the security level of the event, the user may have to provide personal identification information to verify the identity of the user prior to receiving the event access information. The method can be performed by a computer program, such as middleware, embodied in a computer readable medium wherein each step is implemented as one or more code segments.

Summary of Invention Paragraph:
[0015] In addition, the present invention provides a method for granting access to an event for a user of an apparatus containing a communications interface, a biometric sensor, a memory and a processor. The method includes the steps of receiving access information and an indication that the user is authorized to use the apparatus from the communications interface, determining whether the access information indicates that access ~~rights to the~~ event are associated with the apparatus, and granting access to the event whenever the access information indicates that access rights ~~to the~~ event are associated with the apparatus. The user is authori~~zed to use the apparatus whenever the apparatus~~ determines that authentication data received from the biometric sensor is valid for the user. The method can be performed by a computer program, such as middleware, embodied in a computer readable medium wherein each step is implemented as one or more code segments.

20

Summary of Invention Paragraph:
[0016] Moreover, the present invention provides a system having one or more user devices, one or more system interfaces operable to communicate with the user device and a system processor communicably coupled to the one or more system interfaces. Each user device includes a substrate, a communications interface disposed within the substrate, a biometric sensor mounted on the substrate, a memory disposed within the substrate, ~~event access information stored in~~ the memory and a device processor disposed within the substrate and communicably coupled to the communications interface, the biometric sensor and the memory. The device processor is operable to process biometric information received from the biometric sensor to verify that a ~~user is authorized to use the apparatus and transmit the event access~~ information and an indication that the user is authorized to use the user device when the user is verified. The user device also includes a power source disposed within the substrate and electrically connected to the communications interface, the biometric sensor and the device processor.

Brief Description of Drawings Paragraph:
[0021] FIG. 4A depicts the front of an exemplary embodiment of a card for enabling transactions using a biometrically enabled programmable magnetic stripe in accordance with the present invention;

Brief Description of Drawings Paragraph:
[0022] FIG. 4B depict the back of an exemplary embodiment of a card for enabling transactions using a biometrically enabled programmable magnetic stripe in accordance with the present invention;

Brief Description of Drawings Paragraph:

[0025] FIG. 6 depicts an exemplary embodiment of the combined elements of a biometrically enabled programmable magnetic stripe on a device for secure physical and commercial transactions in accordance with the present invention;

Brief Description of Drawings Paragraph:
[0027] FIG. 8 depicts one embodiment of an exemplary device for effecting secure physical and commercial transactions in a contactless manner using biometrics identity validation in accordance with the present invention;

Brief Description of Drawings Paragraph:
[0030] FIG. 11 is a diagram illustrating another embodiment of an exemplary device for effecting secure physical and commercial transactions in a contactless manner using biometrics identity validation in accordance with the present invention;

Brief Description of Drawings Paragraph:
[0031] FIG. 12 is an illustration of one embodiment of a biometric sensor that may be used in the device of FIG. 11 in accordance with the present invention;

Brief Description of Drawings Paragraph:
[0032] FIG. 13A illustrates various layers that form one embodiment of the biometric sensor of FIG. 12 in accordance with the present invention;

Brief Description of Drawings Paragraph:
[0039] FIG. 19 is flow chart of an exemplary method for storing a biometric template analog in the device of FIG. 8 in accordance with the present invention;

Detail Description Paragraph:
[0047] To remedy the deficiencies of existing systems and methods, the present invention provides a system, method and apparatus for securely granting access to an event. For example, in one embodiment of the present invention, an apparatus, such as an electronic card, ticket or information carrier, contains validated biometric data about a user. When the "ticket" is purchased or authenticated, event access information is stored on the electronic card or ticket by an entity authorized by the event provider. The user is allowed access to the event when the biometric data stored on the electronic card or ticket matches the user's biometric data and the event access information is validated. The user's biometric data is authenticated via a biometric sensor on the electronic card or ticket. The user's biometric data can also be authenticated by the entity granting access to the event.

Detail Description Paragraph:
[0049] The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the use of on-card/device biometric authentication of the user and programmable magnetic stripes such that the data within the tracks of the stripe can be manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into the card or device. Alternatively, the data can be stored in the on-card processor/controller and then transmitted via time-varying signal to the card reader thereby emulating the swipe of a magnetic stripe through the magnetic card reader. In addition, the card or device can provide such information via a contactless communication system. These capabilities also enable multiple sets of data and applications to be incorporated onto a single card, device or media, thereby making it a universal card/device with numerous sets of data (e.g., accounts) and/or applications that can be temporarily downloaded onto the magnetic stripe from the memory of the on-card processor, used in the desired application, and then modified or erased. Finally, some or all of the above features can be disabled until the owner of the card enables them through use of an on-card biometrics sensor and logic that is pre-registered to the cardholder. As a result, maximum security is guaranteed since the card cannot be

used if it is lost or stolen, and skimming can be virtually eliminated by prompt modification or erasure of the magnetic stripe data following the basic transaction authorized by the owner.

Detail Description Paragraph:
[0050] Now referring to FIG. 3, a block diagram of a system 300 for enabling transactions in accordance with one embodiment of the present invention is shown. More specifically, the present invention provides a system 300 having one or more user devices 302, one or more system interfaces 304 operable to communicate with the user device(s) 302 and a system processor or controller 306 communicably coupled to the one or more system interfaces 304. Each user device 302 includes a magnetic field generator 308 that is normally inactive, a biometric sensor 310, a memory 312, a device processor or controller 314 and a power source 316. Note that the memory 312 and device processor 314 may be integrated into a single integrated circuit. The device processor 314 may also include a smart card processor and an application specific integrated circuit ("ASIC") chip. In addition, the power source 316 may be controlled by a power management unit 318. The magnetic field generator 308, biometric sensor 310 and memory 312 are all communicably coupled to the device processor 314. The magnetic field generator 308, biometric sensor 310, memory 312 and device processor 314 are all electrically connected to the power source 316 via the power management unit 318. If the user device 302 does not include a power management unit 318, the magnetic field generator 308, biometric sensor 310, memory 312 and device processor 314 will all be electrically connected to the power source 316. The device processor 314 is operable to process biometric information received from the biometric sensor 310 to verify that a user is authorized to use the device 302 and activate the magnetic field generator 308 when the user is verified.

Detail Description Paragraph:
[0052] The biometric sensor 310 may include a fingerprint sensor, retina sensor or voice sensor or other sensor device capable of detecting unique characteristics of a person that can then be compared to stored data. One example of such a fingerprint sensor includes a matrix of points operable to detect high and low points corresponding to ridges and valleys of a fingerprint. Another example of a fingerprint sensor includes an emitter and a detector wherein light projected by the emitter is reflected from a user's finger onto the detector.

Detail Description Paragraph:
[0053] When the device 302 is initialized or linked to a user, the biometric sensor 310 is used to collect biometric information about the user. This biometric information is stored as a biometric analog of the user in the memory 312. Thereafter, and as will be described below in reference to FIG. 7, biometric information or authentication data is obtained by the biometric sensor 310 and sent to the device processor 314 for authentication. The device processor 314 determines whether the authentication data is valid for one of the users by comparing the authentication data to the biometric template stored in memory 312. If the authentication data is valid, the device processor 314 activates the magnetic field generator 308 and provides binary data to the magnetic field generator 308 to be transmitted as a magnetic signal. The magnetic field generator 308 then generates the magnetic signal corresponding to the information associated with the authenticated user and the selected application. The device processor 314 will then deactivate the magnetic field generator 308 after the magnetic field generator 308 has been active for a specified period of time. Alternatively, the device processor 314 may deactivate the magnetic field generator 308 when the biometric sensor 310 no longer detects the authorized user, or a transaction complete signal is received. The present invention reduces power consumption of the device 302 and increases security by (1) keeping the magnetic field generator 308 normally inactive, (2) activating the magnetic field generator 308 and transmitting the magnetic signal only after the user has been authenticated, and (3) disabling the magnetic field generator sometime thereafter. Additional power consumption can be

reduced by keeping the device 302 in a sleep or low power mode until certain activation parameters have been satisfied, such as receiving an external signal, contact with the biometric sensor 310 or a user input/command.

Detail Description Paragraph:
[0056] The components of the device 302 are typically disposed within or mounted on a substrate. For example, the biometric sensor 310, user interface 320, smart card interface 324 and optical or other I/O interface 326 are typically mounted on the substrate; whereas the memory 312, device processor 314, power source 316 and power management unit 318 are typically disposed within the substrate. The magnetic field generator 308 and contactless interface 322 can be mounted on the substrate or disposed within the substrate. The type of material used for the substrate and the resulting properties of the substrate will depend on the desired application and working environment for the device 302. In many cases, the substrate will be a semi-flexible material, such as plastic, or a laminate material. The substrate can then be integrated into a card, such as an access card, a credit card, a debit card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card, etc. The substrate may also be integrated into a travel credential, such as a passport, an immigration card and a visa, etc. In addition, the substrate may be integrated into a personal communication device, such as a personal data assistant (PDA), a telecommunications device, a pager, a computer and an electronic mail transceiver, etc. Moreover, the substrate may be integrated into a personal device/belonging, such as a watch, a jewelry, a key ring, a tag and eye glasses, etc.

Detail Description Paragraph:
[0058] Referring now to FIG. 4A, the front 400 of an exemplary embodiment of a card for enabling transactions using a biometrically enabled programmable magnetic stripe in accordance with the present invention is shown. The card is shown in the form of a credit or debit card, but may also be used as an access card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card, etc. The front 400 of the card includes the issuer's name 402, a biometric sensor 310, a photo or I/O interface 404 (user interface 320 or other I/O interface 326), a smart card interface 324, a card number 406, an expiration date 408, the card holder's name 410 and a hologram 412. Other information and features may also be placed on or within the card. As will be appreciated by those skilled in the art, the features described above can be rearranged or eliminated to fit a specific application for the card.

Detail Description Paragraph:
[0059] Now referring to FIG. 4B, the back 450 of an exemplary embodiment of a card for enabling transactions using a biometrically enabled programmable magnetic stripe in accordance with the present invention is shown. The back 450 of the card includes the magnetic field generator 308 (programmable magnetic stripe), an area for the card holder to place an authorized signature 452 and the issuer's contact information and disclaimers 454. Other information and features may also be placed on or within the card. As will be appreciated by those skilled in the art, the features described above can be rearranged or eliminated to fit a specific application for the card.

Detail Description Paragraph:
[0061] Now referring to FIG. 5B, a block diagram of a programmable magnetic stripe 550 (308 FIG. 3) using a single induction coil 552 for sending emulated time-varying magnetic stripe data to a magnetic card reader directly from the on-card controller in accordance with another embodiment of the present invention is shown. The programmable magnetic stripe 550 (308 FIG. 3) includes a magnetic stripe 502, a single inductive coil 552 and a control circuit 554. The magnetic stripe 502 contains one or more sets of magnetic data cells 504-516. For example, magnetic stripe 502 will typically contain three tracks or sets of magnetic data cells 504-516. The long inductive coil 552 is mounted immediately beneath the entire length

of the magnetic stripe 502 and its corresponding binary magnetic data cells 504-516 such that a time-varying signal can be transmitted to the heads of the magnetic card reader as the card is swiped through the reader. The data rate is determined based on the minimum and maximum swipe speeds that standard readers can accommodate. In other words, the single inductive coil 552 is long enough for it to be in the physical proximity of the card reader heads for the entire time period required to transmit the time-varying signal from the card to the card reader. The inductive coil 552 is electrically connected to the control circuit 554, which may be integrated into the device processor 314 (FIG. 3). By establishing the configuration in this manner, the inductive coil 552 can be pulsed with varying currents and current directions so that the time-varying data stream of a card being swiped through the reader is emulated, thus providing the same magnetic data stream to the reader heads of the magnetic stripe reader as would be seen if a card with binary data in multiple spatially distributed data cells 504-516 in the magnetic stripe 502 were swiped through the reader. This magnetic signal will, therefore, emulate the data that would be generated by the swipe of a magnetic stripe card with the desired information embedded in the individual data cells 504-516 of the stripe 502.

Detail Description Paragraph:
[0062] Note that the individual data cells 504-516 are normally empty of data. There are several ways in which the card can be activated so that the data transfer can be started. For example, the card can be initially activated by the authorized user using an on-card "enable button", such as a low-power capacitance sensor, that can be built into the ring of the biometrics sensor 302 (FIG. 3) and used to "wake up" the card when the user is ready to authenticate himself/herself and begin using the card. Authentication of the card user is time stamped for use in determining the length of time to allow transmission of the emulated data. In addition, the magnetic reader 330 (FIG. 3) may have a start sentinel that signals a detector on the card to alert the card that it is in the presence of the card reader 330 (FIG. 3). Once the card is alerted that it is being swiped through the reader 330 (FIG. 3), it begins transmission of the emulated time-varying data from the device processor to the inductive coils 552, thereby generating an exact emulation and transmission to the reader 330 (FIG. 3) of the data that would have been produced by swiping the card through the reader 330 (FIG. 3) with spatially varying data included in the individual data cells 504-516. All such transmission of emulated card data is contingent upon valid biometric authentication of the card user, followed by detection of the card that it is in the presence of the reader head and the reader 330 (FIG. 3) has recognized the start sentinel on the card so that the reader 330 (FIG. 3) is ready to accept the stream of emulated data provided by the device processor. The transmission of data from the device processor 314 (FIG. 3) is suspended once the initial reading of data by the magnetic card reader 330 (FIG. 3) has been completed. This action prevents skimming of card information after the basic transaction has been completed.

Detail Description Paragraph:
[0063] Referring now to FIG. 6, a programmable magnetic card 600 is equipped with inductive coils as illustrated in FIGS. 5A or 5B. An on-card biometrics sensor 310 is incorporated to enable positive authentication of the user of the card. This is accomplished by transmitting a biometrics template from the biometrics sensor 310 to the on-card control processor 314 that performs matching operations on the template sent from the biometrics sensor 310 with a template obtained from the authorized user of the card, such authorized template being resident in the control processor 314 (memory 312) from initial registration of the authorized card owner and/or user. Once such biometrics matching has been accomplished, the control processor 314 then authorizes the necessary account numbers and/or card applications to be downloaded into the individual data tracks of the programmable magnetic stripe 308 (magnetic field generator; see also 502 FIGS. 5A and 5B), which then enables the card to be used in standard card-readers throughout the existing world-wide infrastructure.

Detail Description Paragraph:
[0064] Now referring to FIG. 7, a flow chart of an exemplary authentication method 700 for using a device, such as device 300 (FIG. 3), in accordance with the present invention is shown. The device contains information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor. The device can be used to enable any type of transaction, such as an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction. The device is normally in standby or sleep mode as shown in block 702. If one or more activation parameters are satisfied, as determined in decision block 704, the device is switched to active mode in block 708. Otherwise, the device remains in standby mode as shown in block 706. The one or more activation parameters may include detecting data from the biometric sensor (e.g., 310 FIG. 3), detecting an external signal from an interface (e.g., 308, 322, 324, 326 FIG. 3) or receiving data from a user interface (e.g., 320 FIG. 3). If authentication data is not received after the device is switched to active mode, as determined in decision block 710, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If, however, the active mode has not timed out, as determined in decision block 712, the device continues to wait for authentication data to be received until the active period has timed out. If, however, authentication data is received from the biometric sensor, as determined in decision block 710, the authentication data is verified in block 716. The verification process determines whether the authentication data is valid for one of the users by comparing the authentication data with a stored biometric template of the one or more users that are authorized or registered to use the device. If the authentication data is not valid, as determined in decision block 718, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If, however, the active mode has not timed out, as determined in decision block 712, the device will again wait for authentication data to be received until the active period has timed out.

Detail Description Paragraph:
[0065] If, however, the authentication data is valid, as determined in decision block 718, the information associated with the authenticated user is accessed in block 720 and provided to the device outputs in block 722. The information can be a simple approval or denial of the transaction, or private information of the user that is required to enable or complete the transaction. As previously described in reference to FIG. 3, the device outputs may include a magnetic field generator 308 (programmable magnetic stripe), a contactless interface 322, a smart card interface 324, or an optical or other I/O interface 326. Using the magnetic field generator 308 for example, this step would involve activating the magnetic field generator 308 and generating a magnetic signal corresponding to the information associated with the authenticated user. In addition, the authentication step (block 716), the information access step (block 720) or the information output step (block 722) may also display information to the user, allow the user to select the information to enable the transaction or allow the user to select the device output or interface to be used. Once the transaction is complete, as determined in decision block 724, the information is cleared from the device output(s) in block 728, the device is switched to standby mode in block 714 and the device waits for various activation parameters in block 704. If, however, the transaction is not complete, as determined in decision block 724 and the process has not timed out, as determined in decision block 726, the process continues to wait for the transaction to be completed. If the process has timed out, as determined in decision block 726, the information is cleared from the device output(s) in block 728, the device is switched to standby mode in block 714 and the device waits for various activation parameters in block 704. The process can be set to interrupt the transaction and deny it if the process times out (e.g., the magnetic field generator has been active for a specified period of time) or the biometric sensor no longer detects

the authorized user. Note that this method can be performed by a computer program, such as middleware, embodied in a computer readable medium wherein each step is implemented as one or more code segments, all of which are performed on the card/device.

Detail Description Paragraph:
[0066] Referring now to FIG. 8, one embodiment of an exemplary device 800 for effecting secure physical and commercial transactions in a contactless manner using biometrics is shown. As will be described later in greater detail, the device 800 includes multiple components, such as a biometric sensor 802, a radio frequency ("RF") antenna 804, a controller 806, control buttons 808, a dynamic information display 810, a magnetic information media component 812, and a RF power conversion and power management unit 814. A number of inter-component communications paths 816 provide connections between various components of the device 800.

Detail Description Paragraph:
[0068] The biometric sensor 802 is used for sensing a physical attribute of a user of the device 800 and generating an analog of this physical attribute. The analog may then be made available to the controller 806. More specifically, the biometric sensor 802 is designed to sense some physical attribute of a person and extract a distinctive analog of that person. To be useful for establishing positive identification, the analog may need to be individualized sufficiently so as to be unique to every person. In addition, a trusted copy--a template--of the analog should be captured. Analogs later sensed by the biometric sensor 802 may then be compared against the template analog. Various physical attributes may be used for identification purposes, such as fingerprints, voice prints, and retinal or iris prints.

Detail Description Paragraph:
[0069] The controller 806 interacts with the biometric sensor 802 and other components of the device 800 to perform various functions. For example, the controller 806 may capture the analog of the physical attribute for long term storage as a trusted template analog of an authorized user, as well as for immediate comparison to a stored trusted template analog during an authentication procedure. The controller 806 may also determine whether the comparison indicates a match between the template analog and the analog captured by the biometric sensor 802. In addition, the controller 806 may control the dynamic information display 810, respond to input from the control buttons 810, and control the magnetic information media component 812. Furthermore, the controller 806 may support two-way communications with an associated reader/writer device (FIG. 9) via the RF antenna 804. The controller may be a single controller/processor or may comprise multiple controllers/processors.

Detail Description Paragraph:
[0073] Referring to FIG. 10 and with continued reference to FIGS. 8 and 9, the device 800 may be operated in the environment 900 using a method 1000 as follows. In step 1002, the device 800 is placed into the RF field 906 emanated by the reader/writer device 902. When placed into the RF field, the device 800 captures power from the RF field 906, which powers up the device's 800 electronics. In step 1004, the biometric sensor 802 is actuated by a user. The method of actuation may depend on the type of biometric sensor (e.g., a fingerprint for a fingerprint sensor, speaking for a voice sensor, etc.). In step 1006, an authentication process is performed by the device 800. As in the previous step, the authentication process may depend on the type of biometric sensor. For example, the detected fingerprint or voice may be compared to a template in the memory of the device 800. In step 1008, a determination is made as to whether the user is authenticated. If the authentication process fails to validate the user, the method 1000 may return to step 1004. If the user is validated by the authentication process, the method continues to step 1010, where the device 800 continues the desired transaction with the reader/writer device 902. Once this occurs, the device 800 may be removed from

the RF field 906 in step 1012, which powers down the device 800.

Detail Description Paragraph:
[0086] Referring now to FIG. 13B, one embodiment of a portion of the device 1100 illustrates the biometric sensor 1102, display 1112, and RF antenna 1104 formed on the substrate 1324. The biometric sensor includes layers 1302-1322 as described with respect to FIG. 10, the display 1112 comprises layer 1326-1336, and the RF antenna comprises layers 1338-1348. As is illustrated in FIG. 13B, each of the components 1102, 1112, 1104 share a number of layers (e.g., 1322, 1336, and 1348). This sharing simplifies the design of the device 1100 and may also reduce manufacturing costs.

Detail Description Paragraph:
[0108] Referring specifically to FIG. 19, before the device 800 is usable in financial transactions, it should be initialized by the buyer/owner with the registration of a selected fingerprint pattern into secured memory of the device 800. To register a selected fingerprint, the device owner holds the device 800 in the RF field generated by a point of sale ("POS") device, which may be a kiosk, personal computer, cash register, or similar device. The RF energy from the POS device provides for the power of the device 800 and display activation in step 1902. In step 1904, a determination is made as to whether the device 800 has been previously used. For example, the device 800 may determine if a fingerprint template analog is already stored in memory. If the device 800 has been previously used, the method 1900 ends. If the device has not been previously used, the device 800 continues to step 1906, where the owner is prompted to actuate the biometric sensor. For example, this may entail the owner briefly touching the biometric sensor 802 on the device 800 with a selected finger or thumb. Note that depending on the intended use of the device 800, the owner may be required to confirm or validate his or her identity and/or security clearance. The fingerprint information is read from the biometric sensor 802 and stored in the device 800 in steps 1908, 1910 while the owner maintains contact with the biometric sensor 802. The owner may maintain contact with the biometric sensor 802 until, in step 1912, an acknowledgement is displayed on the display 800 that the fingerprint pattern has been successfully registered in the device 800 as an encrypted template.

Detail Description Paragraph:
[0109] Referring specifically to FIG. 20, to authorize a payment transaction where invoice information is displayed by the POS device, the user of the device 800 holds the device 800 within a RF field generated by a RF reader connected to the POS device in step 2002. For example, the user may hold the device 810 at an approximate six inch distance from the RF reader. In step 2004, the user actuates the biometric sensor 802 (e.g., touches the fingerprint sensor with his/her finger or thumb) to effect a comparative match with his/her previously registered fingerprint securely stored in the memory of the card. A successful match effects an encrypted approval and transfer of cardholder account data to the seller's administrative account receivables processing system.

Detail Description Paragraph:
[0111] Now referring to FIGS. 21-23, the present invention will be described in reference to electronic ticketing. For example, FIG. 21 illustrates a flowchart of an authentication process 2100 in accordance with one embodiment of the present invention. In this embodiment, a user initially acquires an access card, electronic ticket, smart card, user device or other such information carrier (see e.g., FIGS. 4A, 4B, 6, 8 and 11) from a central distribution site. The smart card is preloaded with the user's identifying information (e.g., fingerprint), a unique identifier code ("UIC"), ticket information, and/or validity information. This information can also be stored at a central database; although in one embodiment, the identifying information is only stored on the smart card after registration of the biometric data (e.g., fingerprint) on the smart card has been validated. For example, an agent at an airline ticket counter authenticates the identity of the user by

examining the user's government issued ID card before storing the identifying information on the smart card.

Detail Description Paragraph:
[0113] If the smart card is determined to be invalid in decision block 2115, the user is denied access to the event in block 2120, and the user can be given another chance to present the smart card in block 2105. If, however, the smart card is determined to be valid, as determined in decision block 2115, identifying information (e.g., fingerprint, palm print, retinal scan, voice print, etc.) is acquired from the user in block 2125. This acquired identifying information or biometric data is compared against the identifying information stored on the smart card to determine if the two sets of information match in decision block 2135. When the identifying information stored on the smart card matches the identifying information acquired by the reader, the user's identity is verified in block 2140 and, if appropriate, access granted to the event. Alternately, when identity is verified, services can be provided to the user. For example, Internet purchasing can be enabled, Internet-based voting can be enabled, government benefits (e.g., WIC, food stamps) can be used, driver's licenses can be verified.

Detail Description Paragraph:
15 [0117] In addition to the smart card reader 2205, the authentication module 2200 includes a fingerprint sensor 2210 (although it could be any type of identity sensor.) The fingerprint sensor 2210 is configured to read the user's fingerprint and verify that the read fingerprint matches the fingerprint data read from the smart card. Assuming that the fingerprints match, an approval indicator can be displayed on the LCD display 2220 and/or LEDs 2215. Alternatively, the LCD display 2220 and the LEDs 2215 can be used to indicate an error in reading the data or an incorrect match of fingerprints--thereby prompting the user to reinsert the smart card and/or to reprovide his fingerprint to the fingerprint sensor.

Detail Description Paragraph:
[0124] Referring now to FIG. 24, a block diagram of an electronic ticketing system 2400 in accordance with one embodiment of the present invention is shown. As previously described, the electronic ticketing system 2400 relies on a user device 2402, which has been previously described as an access card, electronic ticket, smart card, user device or other such information carrier (see e.g., FIGS. 4A, 4B, 6, 8 and 11). The user device 2402 is an apparatus that includes a substrate, a communications interface disposed within the substrate, a biometric sensor mounted on the substrate, a memory disposed within the substrate, event access information 2406 stored in the memory and a processor disposed within the substrate that is communicably coupled to the communications interface, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and transmit the event access information 2406 and an indication that the user is authorized to use the apparatus via the communications interface when the user is verified. A power source is also disposed within the substrate and electrically connected to the communications interface, the biometric sensor and the processor. The communications interface may include a wireless transceiver, an optical transmitter, a magnetic stripe, a programmable magnetic stripe or magnetic field generator that is normally inactive, a smart card interface or communications port. The magnetic field generator can create a spatial magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader.

Detail Description Paragraph:
[0125] The user of the device 2402 purchases a ticket or obtains authorization to access an event from a ticket purchase or authentication station 2404. In some cases, such as with airlines or restricted area access, the user will present various forms of personal identification before the event access information 2406

will be provided. In other words, the user provides personal identification information to verify the identity of the user prior to receiving the event access information. The user may also have to validate that he or she is the authorized user of the device 2402 using the biometric sensor on the device 2402 as previously described (e.g., personal ID information checked against registered biometric data). On the other hand, such as for a concert, the user may only have to purchase the ticket. The ticket purchase or authentication station 2404 will provide or deny the event access information 2406 based on local information or on information obtained or verified using the system processor 2408 and/or other external systems 2410, such as state and federal databases. Once the user is properly validated, the event access information 2406 is transmitted to the user device 2402 where it is stored in memory. The event access information 2406 may be encrypted or otherwise coded to prevent fraudulent use or copying of the event access information 2406.

Detail Description Paragraph:
[0126] The user attempts to gain access to the event by validating that he or she is the authorized user of the device 2402 using the biometric sensor on the device 2402 as previously described. If the user is authenticated, the user device 2402 transmits the event access information and user validation 2412 to the event access station 2414. The user validation is an indicator that the user is authorized to use the device 2412. The event access station 2414 validates the event access information 2406 either locally or via system processor 2408. If the event access information 2406 is valid, the user is granted access to the event. Otherwise, the user may retry to gain access with the device 2402, or try to authenticate his or her association to the event access information 2406 via external biometric sensors or other identification means, or be subject to further security checks/inquiry. Note that the device 2402 may also transmit an indication that the user is not authorized to use the device 2402 when the user is not properly authenticated.

Detail Description Paragraph:
[0127] As a result, the present invention provides a system having one or more user devices 2402, one or more system interfaces 2404 and 2414 operable to communicate with the user device 2402 and a system processor 2408 communicably coupled to the one or more system interfaces 2404 and 2414. Each user device 2402 includes a substrate, a communications interface disposed within the substrate, a biometric sensor mounted on the substrate, a memory disposed within the substrate, event access information 2406 stored in the memory and a device processor disposed within the substrate and communicably coupled to the communications interface, the biometric sensor and the memory. The device processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and transmit the event access information 2406 and an indication that the user is authorized to use the user device 2402 when the user is verified. The user device 2402 also includes a power source disposed within the substrate and electrically connected to the communications interface, the biometric sensor and the device processor. The one or more system interfaces 2404 and 2414 may include an optical interface, a smart card interface, a wireless communication interface, a magnetic reader, an initialization interface, a recharger or other communication port. A database may be communicably coupled to the system processor 2408. Moreover, one or more remote computers or external systems can be communicably coupled to the system processor 2408 via one or more networks or direct connections.

Detail Description Paragraph:
[0128] Now referring to FIGS. 25A, 25B and 25C, flowcharts illustrating various methods of operation of an electronic ticketing system in accordance with one embodiment of the present invention are shown. FIG. 25A illustrates the process 2500 to validate the user and provide the event access information to the user device. The process starts by determining the identity and access rights of a user to the event in block 2502. This may include purchasing the ticket, providing a photo ID, providing biometric information or undergoing a security or background

check. If access is to be granted, as determined in decision block 2504, the event access information 2406 is created in block 2506. The event access information is then transmitted to the user device via the communication interfaces (physical or wireless) and stored in the memory of the user device in block 2508. The access information can be encrypted or otherwise coded to prevent unauthorized use of the information. If, however, access is not to be granted, as determined in decision block 2504, access to the event is denied in block 2510 and various checks can be made on the user device or the security rating of the user in block 2512. The method can be performed by a computer program, such as middleware, embodied in a computer readable medium wherein each step is implemented as one or more code segments.

Detail Description Paragraph:
[0129] FIG. 25B illustrates the process 2530 to request access to an event using the user device. The process starts by receiving event access information from an external source via the communications interface and storing the access information in the memory in block 2532. Authentication data is then received from the biometric sensor in block 2534 as previously described for on-card biometric authentication. If the authentication data is valid for the user, as determined in decision block 2536, access to the event is requested by transmitting the event access information and an indication that the user is authorized to use the apparatus via the communications interface in block 2538. If, however, the authentication data is not valid, as determined in decision block 2536, the event access information is not transmitted in block 2540. Alternatively, a access denial indication can be transmitted. The method can be performed by a computer program, such as middleware, embodied in a computer readable medium wherein each step is implemented as one or more code segments.

Detail Description Paragraph:
[0130] FIG. 25C illustrates the process 2560 for granting access to an event. The process 2560 starts by receiving access information and an indication that the user is authorized to use the apparatus from the communications interface in block 2562. If the event access information is valid (e.g., access information indicates that access rights to the event are associated with the apparatus), as determined in decision block 2564, access to the event is granted in block 2566. If, however, the event access information is not valid, as determined in decision block 2564, the user is denied access to the event in block 2568 and additional device or security checks can be performed in block 2570. The user is authorized to use the apparatus whenever the apparatus determines that authentication data received from the biometric sensor is valid for the user. The method can be performed by a computer program, such as middleware, embodied in a computer readable medium wherein each step is implemented as one or more code segments.

CLAIMS:

1. An apparatus comprising: a substrate; a communications interface disposed within the substrate; a biometric sensor mounted on the substrate; a memory disposed within the substrate; event access information stored in the memory; a processor disposed within the substrate and communicably coupled to the communications interface, the biometric sensor and the memory, wherein the processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and transmit the event access information and an indication that the user is authorized to use the apparatus via the communications interface when the user is verified; and a power source disposed within the substrate and electrically connected to the communications interface, the biometric sensor and the processor.

14. The apparatus as recited in claim 1, wherein the biometric sensor is selected from the group consisting of a fingerprint sensor, retina sensor, iris sensor or voice sensor.

15. The apparatus as recited in claim 1, wherein the biometric sensor comprises a matrix of points operable to detect high and low points corresponding to ridges and valleys of a fingerprint.

16. The apparatus as recited in claim 1, wherein the biometric sensor comprises an emitter and a detector wherein light projected by the emitter is reflected from a user's finger onto the detector.

25. The apparatus as recited in claim 1, wherein the memory contains a biometric analog of a user.

26. The apparatus as recited in claim 3, wherein the processor provides binary data to the magnetic field generator after a user has been authenticated using the biometric sensor.

28. The apparatus as recited in claim 3, wherein the processor deactivates the magnetic field generator when the biometric sensor no longer detects the authorized user.

29. A method for requesting access to an event by a user of an apparatus containing communications interface, a biometric sensor, a memory and a processor, the method comprising the steps of: receiving event access information from an external source via the communications interface and storing the event access information in the memory; receiving authentication data from the biometric sensor; determining whether the authentication data is valid for the user; and requesting access to the event by transmitting the event access information and an indication that the user is authorized to use the apparatus via the communications interface whenever the authentication data is valid.

35. The method as recited in claim 34, wherein the one or more activation parameters includes detecting data from the biometric sensor, detecting an external signal or receiving data from a user interface.

36. The method as recited in claim 29, wherein the step of determining whether the authentication data is valid comprises comparing the authentication data to one or more biometric templates stored on the apparatus.

40. A computer program embodied in a computer readable medium for requesting access to an event by a user of an apparatus containing communications interface, a biometric sensor, a memory and a processor, the computer program comprising: a code segment for receiving event access information from an external source via the communications interface and storing the event access information in the memory; a code segment for receiving authentication data from the biometric sensor; a code segment for determining whether the authentication data is valid for the user; and a code segment for requesting access to the event by transmitting the event access information and an indication that the user is authorized to use the apparatus via the communications interface whenever the authentication data is valid.

41. A method for granting access to an event for a user of an apparatus containing communications interface, a biometric sensor, a memory and a processor, the method comprising the steps of: receiving event access information and an indication that the user is authorized to use the apparatus from the communications interface, wherein the user is authorized to use the apparatus whenever the apparatus determines that authentication data received from the biometric sensor is valid for the user; determining whether the event access information indicates that access rights to the event are associated with the apparatus; and granting access to the event whenever the event access information indicates that access rights to the event are associated with the apparatus.

46. A computer program embodied in a computer readable medium for granting access to an event for a user of an apparatus containing communications interface, a biometric sensor, a memory and a processor, the computer program comprising: a code segment for receiving event access information and an indication that the user is authorized to use the apparatus from the communications interface, wherein the user is authorized to use the apparatus whenever the apparatus determines that authentication data received from the biometric sensor is valid for the user; a code segment for determining whether the event access information indicates that access rights to the event are associated with the apparatus; and a code segment for granting access to the event whenever the event access information indicates that access rights to the event are associated with the apparatus.

47. A system comprising: one or more user devices, each user device comprising a substrate, a communications interface disposed within the substrate, a biometric sensor mounted on the substrate, a memory disposed within the substrate, a device processor disposed within the substrate and communicably coupled to the communications interface, the biometric sensor and the memory, wherein the processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and the event access information and an indication that the user is authorized to use the apparatus via the communications interface when the user is verified, and a power source disposed within the substrate and electrically connected to the communications interface, the biometric sensor and the device processor; one or more system interfaces operable to communicate with the user device; and a system processor communicably coupled to the one or more system interfaces.

Previous Doc Next Doc Go to Doc#

Refine Search

Search Results -

Terms	Documents
L1 and (cpu or computer)	1

Database:

US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L14

Refine Search

Recall Text Clear Interrupt

Search History

DATE: Tuesday, July 12, 2005 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
	DB=PGPB,USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L14	L1 and (cpu or computer)	1	L14
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L13	L1 and (indicat$ or screen$ or monitor$)	1	L13
	DB=PGPB,USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L12	L11 and screen	1	L12
L11	(L9 or 11) and ((authenticat$ or verif$) and (biometr$ or facial$ or print$ or finger$ or iris$))	2	L11
L10	L9 and ((authenticat$ or verif$) same (biometr$ or facial$ or print$ or finger$ or iris$))	1	L10
L9	L5 or l4	15	L9
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR		
L8	(l1 or l6) and ((authenticat$ or verif$) and (biometr$ or facial$ or print$ or	1	L8

	iris$))		
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L7	(l1 or l6) and ((authenticat$ or verif$) same (biometr$ or facial$ or print$ or iris$))	1	L7
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR		
L6	(2003/0055541 | 2001/0026316 | 5686765 | 2003/0062447 | 4390861 | 2003/0050745 | 4586387 | 2002/0111777 | 5938706 | 2762992 | 5067674 | 2003/0055540 | 2620148 | 2003/0052798 | 5479162 | 4914721 | 2003/0093193 | 2002/0093565 | 6311272 | 2002/0035415 | 6584383 | 3082978 | 6348877)![PN] and ((authenticat$ or verif$) same (biometr$ or facial$ or print$ or iris$))	1	L6
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L5	(2003/0055541 | 2001/0026316 | 5686765 | 2003/0062447 | 4390861 | 2003/0050745 | 4586387 | 2002/0111777 | 5938706 | 2762992 | 5067674 | 2003/0055540 | 2620148 | 2003/0052798 | 5479162 | 4914721 | 2003/0093193 | 2002/0093565 | 6311272 | 2002/0035415 | 6584383 | 3082978 | 6348877)![PN]	13	L5
L4	('6810310'| '6691956')[PN]	2	L4
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR		
L3	('6810310'| '6691956')[URPN] and ((authenticat$ or verif$) same (biometr$ or facial$ or print$ or iris$))	0	L3
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L2	('6810310'| '6691956')[URPN]	2	L2
L1	6810310.pn. or 6691956.pn.	2	L1

END OF SEARCH HISTORY

L11: Entry 2 of 2 File: USPT Nov 26, 1991

DOCUMENT-IDENTIFIER: US 5067674 A
TITLE: Control system for remote controlled aircraft

Detailed Description Text (14):
The substructure may also advantageously be equipped with an adaptation module DRIVER.sub.s permitting assurance of the compatibility between the module UART.sub.s and a personnel computer PC.sub.2 intended for verification tests. This module DRIVER.sub.s may be of the "MAX 239" type. The computer PC.sub.s may be used for controlling the quality of the hertzian bundle with the on-board apparatus (extraction of statistical parameters such as the percentage of messages to repeat, the percentage of errors . . .).

Detailed Description Text (17):
Further, a series/parallel communication module SER/PAR is connected to the BUS.sub.s for achieving exchanges of data between the central unit ALU.sub.s and the peripherals, in particular the personal computer PC.sub.1, the pocket terminal TERM, the printer PRN, the host computer HOST. This SER/PAR module is essentially comprised of a multiprotocol communication processor, address decoders for reading and writing in the specialized registers of the communication processor, and adaptation modules (analogous to the DRIVER.sub.s module already mentioned). This module permits complete integration of the system described with conventional information processing for a control or an action on this system. For example, a bank of geographic data may be consulted by the computer HOST in order to constitute a file of trajectories, this being remotely loaded into the on-board apparatus via the substructure on the ground. The personnel computer PC.sub.1 may permit a digital visualization of the altitude data of the aircraft.

Detailed Description Text (29):
The on-board apparatus may advantageously be equipped with an adaptation module DRIVER.sub.em permitting assuring the compatibility between a UART.sub.em module and a personal computer PC.sub.3 for verification tests when the aircraft is on the ground. This module is particularly of the "MAX 239" type. The computer PC.sub.3 may be used for controlling the quality of the hertzian bundle with the substructure on the ground, for carrying out a control of the operation of the different systems of the aircraft.

Detailed Description Text (56):
The message received on the ground by the unit UART.sub.s (via the units HF.sub.s and MODEM.sub.s) releases an algorithm situated in the unit ROM.sub.s which displaced the result of the measurements in the unit RAM.sub.s ; the result is then sent to the multiprotocol communication unit SFR/PAR to be able to be interpreted for the peripherals HOST, PCI, TERM, PRN, in order to be displayed on the screen or printer.

CLAIMS:

1. A system for controlling a remote controlled aircraft equipped with servomotors for carrying out different functions, said system comprising a substructure for

piloting from a distance and an on-board apparatus mounted on the aircraft,

said piloting substructure comprising:

a piloting console (CP) adapted to deliver analog piloting signals,

an analog/digital conversion unit (A/D-PCM) for converting said piloting signals into digital data,

a volatile memory unit (RAM.sub.s) for storing the digital data,

a central computing unit (ALU.sub.s) for carrying out logical operations on the stored data according to predetermined operating programs,

a non-volatile memory unit (ROM.sub.s) containing the operating programs for the central unit (ALU.sub.s),

an asynchronous communication module (UART.sub.s)adapted to transform the data issued from the computing unit into a serial signal, and for converting a serial signal received and loading the corresponding data into an internal register accessible by the central unit (ALU.sub.s),

a modulation/demodulation unit (MODEM.sub.s) adapted to modulate the serial signal issued from the module (UART.sub.s) and demodulate the modulated signals and transmit them to said module (UART.sub.s),

a radio transmitting/receiving module (HF.sub.s) for amplifying and transmitting the modulated signals issued from the unit (MODEM.sub.s) and receiving the modulated signals emitted by the on-board apparatus,

a binary input/output port (DIO.sub.s) driven or controlled by the central unit (ALU.sub.s),

a set of binary actuators and sensors (PANEL) states directed or controlled by the port (DIO.sub.s),

a series/parallel communication module (SER/PAR) adapted to provide exchanges of data between the central unit (ALU.sub.s) and the peripherals, in particular a personal computer (PC.sub.1), a pocket terminal (TERM), a printer (PRN), a host computer (HOST),

said on-board apparatus comprising:

a radio transmitting/receiving module (HF.sub.e), forming with the module (HF.sub.s) a hertzian bundle, and adapted to transmit and receive modulated signals,

a modulation/demodulation unit (MODEM.sub.em) adapted to modulate a serial signal and transmit it to the module (HF.sub.e), and the demodulate the signals coming from this module (HF.sub.e),

an asynchronous communication module (UART.sub.em) adapted to transform data into a serial signal and transmit the same toward the unit (MODEM.sub.e), and for converting the serial signal from the unit (MODEM.sub.e) and loading the corresponding data into an internal register,

a volatile memory unit (RAM.sub.em) for storing the digital data,

a central computing unit (ALU.sub.em) for providing logical operations on the stored data, said unit having access to the internal register of the module

(UART.sub.em),

a non-volatile memory unit (ROM.sub.em) containing the operating programs for the central unit (ALU.sub.em),

a digital/analog conversion unit (D/A-PCM) adapted to generate a composite analog command signal from the data treated by the computing unit,

a demodulator (DEM) adapted to receive the aforementioned composite signal and deliver to each servo-motor of the aircraft a simple analog signal understandable thereby,

a binary input/output port (DIO.sub.me) commanded or controlled by the central unit (ALU.sub.me),

an assembly of binary actuators and sensors (DACT) having states ordered or controlled by the port (DIO.sub.me),

an assembly of sensors (IMAG) comprising in particular inclinometers, a magnetometer, accelerometers, gyrometers, an altimeter, a speed indicator, tachometer, a fuel gauge, alternator load indicator, able to furnish analog signals representative of the position, operation and internal parameters of the aircraft,

a multichannel analog/digital convertor (A/D.sub.e) for converting the analog signals from the sensors (IMAG) into digital data and placing the data into the memory unit (RAM.sub.em),

a universal interface (UPI) for providing exchanges of data between the central unit (ALU.sub.me) and the peripherals (AUX), in particular an auxiliary processor.

3. A ~~control~~ system as in claim 1, characterized in that said remote piloting substructure and ~~said~~ on-board apparatus each comprise an adaptation module (DRIVER.sub.s, DRIVER.sub.em) ~~for assuring~~ compatibility between the communication module (UART.sub.s, UART.sub.me) and a personal computer (PC.sub.2), for test verification.

Previous Doc   Next Doc   Go to Doc#

10/709268

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#

End of Result Set

□ Generate Collection Print

L5: Entry 4 of 4 File: USPT Jul 11, 2000

US-PAT-NO: 6087942
DOCUMENT-IDENTIFIER: US 6087942 A

TITLE: Tactile alert and massaging system

DATE-ISSUED: July 11, 2000

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Sleichter, III; Charles G.	Dana Point	CA		
Cutler; Stanley	Van Nuys	CA		
Gerth; Gayle B.	Dana Point	CA		
Otis, Jr.; Alton B.	Port Townsend	WA		
Chau; Taylor	Cerritos	CA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
JB Research, Inc.	Bellflower	CA			02

APPL-NO: 09/ 081402 [PALM]
DATE FILED: May 18, 1998

INT-CL: [07] G08 B 23/00

US-CL-ISSUED: 340/576; 340/575, 601/49
US-CL-CURRENT: 340/576; 340/575, 601/49

FIELD-OF-SEARCH: 340/575, 340/576, 340/573.1, 340/539, 601/49, 601/86, 601/87, 601/91, 601/90, 601/97, 601/98, 601/101, 601/150, 600/549

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
□	3786628	January 1974	Fossard et al.	
□	3938123	February 1976	Warner	
□	4028882	June 1977	Muncheryan	

□	4059830	November 1977	Threadgill	
□	4203098	May 1980	Muncheryan	
□	4326506	April 1982	Kawabata	
□	4354179	October 1982	Fourcade	
□	4380759	April 1983	Sulkoski et al.	
□	4401971	August 1983	Saito et al.	
□	4779615	October 1988	Frazier	
□	4785280	November 1988	Fubini et al.	340/576
□	5020517	June 1991	Foster, Jr. et al.	128/33
□	5033864	July 1991	Lasecki et al.	600/549
□	5076260	December 1991	Komatsu	
□	5089998	February 1992	Rund	
□	5282181	January 1994	Entner et al.	
□	5429585	July 1995	Liang	601/49
□	5437608	August 1995	Cutler	601/49
□	5462515	October 1995	Tseng	601/57
□	5495242	February 1996	Kick et al.	
□	5581238	December 1996	Chang et al.	340/573
□	5585785	December 1996	Gwin et al.	340/575
□	5684460	November 1997	Scanlon	
□	5686882	November 1997	Giani	
□	5857986	January 1999	Moriyasu	601/49
□	5868687	February 1999	Tedesco	601/49

ART-UNIT: 276

PRIMARY-EXAMINER: Hofsass; Jeffrey A.

ASSISTANT-EXAMINER: La; Anh

ATTY-AGENT-FIRM: Sheldon & Mak

ABSTRACT:

A tactile alert stimulation and massaging system for equipment such as a vehicle includes a pad; a heater element, and motorized vibrators in respective regions of the pad; a plurality of vibratory transducers for location relative to plural zones of the seat, each transducer being responsive to a transducer power signal; a microprocessor controller having program and variable memory and an input and output interface; an array of input elements connected to the input interface for signaling the microprocessor in response to operator input, the signaling including an intensity control value, a plurality of mode signals, and a plurality of region signals relating transducers to be enabled; a driver circuit responsive to the

output interface for producing, separately for each of the transducers, the power signal; and the microprocessor controller being operative in response to the input elements for activating the transducers for operation thereof in a plurality of modes including a massaging mode selectively producing activation of the drive signals at adjustable intensity corresponding to the intensity control value for soothingly massaging muscle groups of the driver; and an alert mode producing a predetermined sequence of alert stimulation cycles, each alert stimulation cycle having an idle portion of between 1 second and 30 seconds, and an active portion of sufficient duration, frequency, and intensity for selectively stimulating the muscle groups of the driver thereby to improve the driver's alertness, wherein successive alert stimulation cycles differ in at least one of intensity, frequency, active portion duration, idle portion duration, and transducers enabled.

41 Claims, 8 Drawing figures

Previous Doc Next Doc Go to Doc#

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#
End of Result Set

□ Generate Collection Print

L5: Entry 4 of 4 File: USPT Jul 11, 2000

DOCUMENT-IDENTIFIER: US 6087942 A
TITLE: Tactile alert and massaging system

Abstract Text (1):

A tactile alert stimulation and massaging system for equipment such as a vehicle includes a pad; a heater element, and motorized vibrators in respective regions of the pad; a plurality of vibratory transducers for location relative to plural zones of the seat, each transducer being responsive to a transducer power signal; a microprocessor controller having program and variable memory and an input and output interface; an array of input elements connected to the input interface for signaling the microprocessor in response to operator input, the signaling including an intensity control value, a plurality of mode signals, and a plurality of region signals relating transducers to be enabled; a driver circuit responsive to the output interface for producing, separately for each of the transducers, the power signal; and the microprocessor controller being operative in response to the input elements for activating the transducers for operation thereof in a plurality of modes including a massaging mode selectively producing activation of the drive signals at adjustable intensity corresponding to the intensity control value for soothingly massaging muscle groups of the driver; and an alert mode producing a predetermined sequence of alert stimulation cycles, each alert stimulation cycle having an idle portion of between 1 second and 30 seconds, and an active portion of sufficient duration, frequency, and intensity for selectively stimulating the muscle groups of the driver thereby to improve the driver's alertness, wherein successive alert stimulation cycles differ in at least one of intensity, frequency, active portion duration, idle portion duration, and transducers enabled.

Application Filing Date (1):
19980518

Brief Summary Text (11):
Typical warning systems of the prior art use visual or auditory indications of sensed conditions for initiating appropriate human responses in the nature of corrective action. For example, vehicle fuel gauges are commonly provided with warning lights that are activated when the supply reaches a low threshold, and aircraft have audible warnings of dangerous conditions such as an impending stall at low speed. Visual indications are often ineffective when used alone, in that they might not be noticed. Auditory indications can be ineffective in noisy environments, particularly when the user is hearing-impaired, and they can be objectionable when the indication does not require immediate corrective action.

Brief Summary Text (16):
In one aspect of the invention, a tactile alert system for an occupant support structure includes a plurality of vibratory transducers for location in plural zones of the support structure; a driver circuit for powering each of the transducers in response to a corresponding drive signal; and a controller responsive to external input for selectively activating the drive signals in a predetermined sequence of alert stimulation cycles of sufficient duration,

frequency, and intensity for selectively stimulating muscle groups of an occupant of the structure, successive alert stimulation cycles differing in at least one of intensity, frequency, and transducers activated, thereby to improve the occupant's alertness.

Brief Summary Text (21):
In another aspect of the invention, a tactile alert system for a user support structure includes a vibratory transducer for location in the support structure; the driver circuit for powering the transducer in response to a drive signal; and the controller responsive to external input for selectively activating the drive signal in a predetermined sequence of alert stimulation cycles of sufficient duration, frequency, and intensity for stimulating muscle tissue of a user of the structure thereby to improve the user's alertness, each alert stimulation cycle having an active portion and an idle portion, wherein successive alert stimulation cycles differ in at least one of intensity, frequency, active portion duration, and idle portion duration. The system can further include a radio receiver having an output for communicating the bodily function input in response to a remote bodily function sensor. The system can further include a sensor unit having a carrier having means for attachment to a body member of the user; a transducer supported by the carrier for generating a sensor signal corresponding to a bodily function of the user, the transducer being selected from the group consisting of a blood pulse sensor, a blood pressure sensor, a body temperature sensor, and an EEG sensor; and a radio transmitter supported by the carrier for communicating the sensor signal to the radio receiver.

Brief Summary Text (24):
and output interface; an array of input elements connected to the input interface for signaling the microprocessor in response to operator input, the signaling including an intensity control value, a plurality of mode signals, and a plurality of region signals relating transducers to be enabled; a driver circuit responsive to the output interface for producing, separately for each of the transducers, the power signal; and the microprocessor controller being operative in response to the input elements for activating the transducers for operation thereof in a plurality of modes including a massaging mode selectively producing activation of the drive signals at adjustable intensity corresponding to the intensity control value for soothingly massaging muscle groups of the driver; and an alert mode producing a predetermined sequence of alert stimulation cycles, each alert stimulation cycle having an idle portion of between 1 second and 30 seconds, and an active portion of sufficient duration, frequency, and intensity for selectively stimulating the muscle groups of the driver thereby to improve the driver's alertness, wherein successive alert stimulation cycles differ in at least one of intensity, frequency, active portion duration, idle portion duration, and transducers enabled.

Detailed Description Text (5):
In some modes of operation, several of the buttons act as double or triple action keys, as further described herein. Specifically, as depicted in FIG. 2, power is turned on or off by a "PWR" button 46 and, when power is supplied, an associated light-emitting diode (LED) 47 is illuminated, the button 46 and the LED 47 being located within an area 48 designated "MASSAGE". The PWR or power button 46 also acts as a double action key for selecting massage duration, and for entering test and demonstration modes that are described below. The four zones 26-32 are individually actuable by pressing corresponding buttons 50, 52, 54, and 56 within a "ZONES" area 60. Visual status indications are provided by respective lights 60L and 60R being disposed adjacent respective buttons or keys 50, 52, 54, and 56 for indicating activation of corresponding left and right ones of the vibrators 12. The heater 16 is operable at two levels by a heat button 62 with corresponding status indications by illumination of an associated LED 63, the button 62 and the LED 63 being within a "HEAT" area 64. The button 62 is a dual action key, sequentially selecting high and low heat levels for the heater 16 as described below.

Detailed Description Text (6):
SELECT, WAVE, PULSE and ZIG-ZAG massaging modes of operation are provided by pressing respective buttons 72, 74, 76, and 78, all enclosed within a modes area 80, SELECT being synonymous with manual operation. The buttons 72, 74, 76 and 78 have respective LEDs 73, 75, 77, and 79 associated therewith for indicating activation if the corresponding modes. "INTENSITY" and "SPEED" adjustments of the massaging modes are provided by the pressing of respective pairs of "+"/"-" switch buttons 96 and 98 within a common area 100. The INTENSITY adjustment relates to the power levels at which the vibratory transducers 12 are driven and, in the case of eccentrically loaded motors also to the frequency of the vibrations. The SPEED adjustment applies to the WAVE, PULSE and ZIG-ZAG modes, and relates to the rate of advancement between mode segments, described below.

Detailed Description Text (13):
Regarding the specific selector keys, the power button 46 is a triple action key that cycles massage power through the states of "off", "on for 15 minutes" and "on for 30 minutes". The LED 47 is preferably bi-color for facilitating indication of the current massage power state. When an "on" state is selected, the massage system 10 will automatically turn off after operating for the selected time period. The first operation of the power button 46 after power is connected results in activation of the select mode described below with zone 1 enabled. In subsequent restartings of the system 10 by the power button 46, the system 10 comes on configured as in the most recent usage.

Detailed Description Text (15):
heat button 62 acts as a triple action key for cycling the heater 16 through the states of "off", "on low" and "on high". The LED 63 indicates the "on low" state by yellow, and the "on high" state by red. When an "on" state is selected, the heater 16 will automatically turn off after 30 minutes. The high state is at full power except as limited by a thermostat that is incorporated in the heater. In the low state, full power is applied for a warmup period of approximately 5 minutes, followed by continued operation at reduced power.

Detailed Description Text (49):
The system status matrix 114 contains the various LED power, heater and mode, zone and control indicators 47, 60L, 60R, 63, 73, 75, 77, 79, 90L, 90C, and 90R. As described above, some of the LED indicators are multiple color devices; they have three terminals in the exemplary configuration described herein, each being connected in the matrix 114 as two separate devices. The system status matrix 114 is configured 4-by-6 and driven in a multiplexed fashion by MPU 110, each "column" of 4 LEDs being activated for about 24% of each display cycle. The period of the complete display cycle is short enough so that all activated indicators appear fully illuminated without any noticeable flicker. Flashing of selected indicators is a function performed by the control firmware independent of the display cycle.

Detailed Description Text (89):
Thus it is believed that the system 10 of the present invention is effective for both improving and maintaining an alertness state of the driver 25, as well as for calling attention to alarm and signal conditions without requiring visual or aural stimulation of the driver. Thus the present invention provides an effective and low cost remedy for alleviating conditions of drowsiness and/or inattention of vehicle and other equipment operators. Suitable vehicles for which the system 10 is appropriate include automobiles, aircraft, trucks, and ships, as well as tractors and other heavy equipment and agri-machinery.

CLAIMS:

22. A vehicle tactile alert system for an operator-driven vehicle having a driver's seat, the system comprising:

(a) a plurality of vibratory transducers for location relative to plural zones of the seat, each transducer being responsive to a transducer power signal;

(b) a microprocessor controller having program and variable memory and an input and output interface;

(c) an array of input elements connected to the input interface for signaling the microprocessor in response to operator input, the signaling including an intensity control value, a plurality of mode signals, and a plurality of region signals relating transducers to be enabled;

(d) a driver circuit responsive to the output interface for producing, separately for each of the transducers, the power signal; and

(e) the microprocessor controller being operative for activating the transducers for operation thereof in a plurality of modes including:

(i) a massaging mode selectively producing activation of the drive signals in response to the input elements at adjustable intensity corresponding to the intensity control value for soothingly massaging muscle groups of the driver; and

(ii) an alert mode producing a predetermined sequence of alert stimulation cycles in response to external input and independently of the intensity control value, each alert stimulation cycle having an idle portion of between 1 second and 30 seconds, and an active portion of sufficient duration, frequency, and intensity for selectively stimulating the muscle groups of the driver thereby to improve the driver's alertness, wherein successive alert stimulation cycles differ in at least one of intensity, frequency, active portion duration, idle portion duration, and transducers enabled.

Previous Doc Next Doc Go to Doc#

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#

End of Result Set

□ Generate Collection Print

L7: Entry 3 of 3 File: USPT Apr 27, 2004

US-PAT-NO: 6727800
DOCUMENT-IDENTIFIER: US 6727800 B1

TITLE: Keyless system for entry and operation of a vehicle

DATE-ISSUED: April 27, 2004

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Dutu; Iulius Vivant	Boca Raton	FL	33496	

APPL-NO: 09/ 982056 [PALM]
DATE FILED: October 18, 2001

PARENT-CASE:
This application claims the benefit of and priority to U.S. application Ser. No. 60/245,026, filed Nov. 1, 2000.

INT-CL: [07] G05 B 19/00

US-CL-ISSUED: 340/5.53; 340/5.6, 340/5.8, 340/5.81, 340/5.82, 340/5.83, 340/5.84, 340/426.11, 340/825.69, 307/9.1, 307/10.2, 307/10.3, 307/10.4, 123/179.1
US-CL-CURRENT: 340/5.53; 123/179.1, 307/10.2, 307/10.3, 307/10.4, 307/9.1, 340/426.11, 340/5.6, 340/5.8, 340/5.81, 340/5.82, 340/5.83, 340/5.84, 340/825.69

FIELD-OF-SEARCH: 340/5.53, 340/5.6, 340/5.65, 340/5.66, 340/5.8, 340/5.81, 340/5.82, 340/5.83, 340/5.84, 340/426.11, 340/5.67, 340/539.1, 340/825.69, 340/825.72, 307/9.1, 307/10.2, 307/10.3, 307/10.4, 307/10.5, 307/10.6, 123/179.1, 361/172

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
□	4158874	June 1979	Ellsberg	361/172
□	4995086	February 1991	Lilley et al.	382/124
□	5337043	August 1994	Gokcebay	340/5.67
□	5661451	August 1997	Pollag	340/426.36

□	5719950	February 1998	Osten et al.	382/115
□	5812067	September 1998	Bergholz et al.	340/5.52
□	5835868	November 1998	McElroy et al.	701/2
□	5903225	May 1999	Schmitt et al.	340/5.25
□	5907286	May 1999	Kuma	340/5.5
□	5917405	June 1999	Joao	340/426.17
□	5982894	November 1999	McCalley et al.	340/5.21
□	5995014	November 1999	DiMaria	340/5.52
□	6021212	February 2000	Ho	29/434
□	6038666	March 2000	Hsu et al.	713/186
□	6078265	June 2000	Bonder et al.	340/5.23
□	6100811	August 2000	Hsu et al.	340/5.83
□	6140939	October 2000	Flick	340/825.69
□	6271745	August 2001	Anzai et al.	340/5.53
□	6542076	April 2003	Joao	340/539

ART-UNIT: 2635

PRIMARY-EXAMINER: Horabik; Michael

ASSISTANT-EXAMINER: DaLencourt; Yves

ATTY-AGENT-FIRM: Malin, Haley & DiMaggio, P.A.

ABSTRACT:

Disclosed is a keyless system for operating and accessing a vehicle such as an automobile, truck, minivan, bus, airplane, train, boat, etc. Preferably, the user's fingerprint is his or her "right of passage" into the vehicle. The system includes fingerprint triggered access to the physical inside space of a vehicle and along with other commands, preferably voice activated and/or card/card reader, control the vehicle's various systems. The system is designed to perform optimally in less than perfect environmental conditions and is preferably provided with its own source of energy. The system also includes a controller and interface in communication with a fingerprint sensor.

30 Claims, 9 Drawing figures

Previous Doc Next Doc Go to Doc#

First Hit Previous Doc Next Doc Go to Doc#

□ Generate Collection Print

L7: Entry 2 of 3 File: PGPB Sep 18, 2003

PGPUB-DOCUMENT-NUMBER: 20030174049
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20030174049 A1

TITLE: Wearable identification appliance that communicates with a wireless communications network such as bluetooth

PUBLICATION-DATE: September 18, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Beigel, Michael L.	Encinitas	CA	US	
Tuttle, John Randall	Boulder	CO	US	
Mosher, Walter W. JR.	West Hills	CA	US	
Wang, David E.	Newport Beach	CA	US	

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	COUNTRY	TYPE CODE
Precision Dynamics Corporation				02

APPL-NO: 10/ 101471 [PALM]
DATE FILED: March 18, 2002

INT-CL: [07] G05 B 19/00, H04 Q 1/00

US-CL-PUBLISHED: 340/10.42; 340/5.61
US-CL-CURRENT: 340/10.42; 340/5.61

REPRESENTATIVE-FIGURES: 2

ABSTRACT:

An identification appliance such as a wristband, headband, armband, ankleband, or legband which has a wireless communication circuit to communicate with a system, network, or device. The identification appliance preferably communicates with a Bluetooth local network and may issue or receive commands or data including voice data. An example command is to expand privileges given to the user of the identification appliance, such as entrance into a restricted area. The information appliance may broadcast its location via a Global Positioning System and have voice activation or speech recognition. The appliance may provide information about the authorized bearer such as his name, address, phone number, passport number, driver's license data, social security number, credit card information, fingerprint data, biometric voice characteristics, retinal characteristics, medical data and so on.

Previous Doc Next Doc Go to Doc#

First Hit Previous Doc Next Doc Go to Doc#

□ Generate Collection Print

L7: Entry 2 of 3 File: PGPB Sep 18, 2003

DOCUMENT-IDENTIFIER: US 20030174049 A1
TITLE: Wearable identification appliance that communicates with a wireless communications network such as bluetooth

Abstract Paragraph:

An identification appliance such as a wristband, headband, armband, ankleband, or legband which has a wireless communication circuit to communicate with a system, network, or device. The identification appliance preferably communicates with a Bluetooth local network and may issue or receive commands or data including voice data. An example command is to expand privileges given to the user of the identification appliance, such as entrance into a restricted area. The information appliance may broadcast its location via a Global Positioning System and have voice activation or speech recognition. The appliance may provide information about the authorized bearer such as his name, address, phone number, passport number, driver's license data, social security number, credit card information, fingerprint data, biometric voice characteristics, retinal characteristics, medical data and so on.

Application Filing Date:
20020318

Detail Description Paragraph:
[0028] The structure 120 may optionally have a closure mechanism to form a circular band. The closure mechanism may make bands of varying or adjustable sizes. Alternatively, the closure mechanism may make the attachment of the identification appliance 100 to a person secure. The secure identification appliance 100 may be configured to make removal or tampering of the identification appliance 100 difficult or impossible. Still, alternatively, a secure identification appliance 100 may have a tamper-evident function; that is, the secure identification appliance 100 may indicate whether tampering of the appliance 100 was attempted. For example, conductive adhesive attachment of areas of the identification appliance 100 upon fastening to the wearer may activate printed conductive patterns within the identification appliance 100 that inform circuitry that the identification appliance 100 has been attached to a wearer or object. If the adhesive attachment of areas of the identification appliance 100 is broken, the printed conductive patterns would detect the break so that the circuit can detect tampering. The configuration and mode of electrical coupling of conductive patterns in the identification appliance 100 to the circuit may vary according to whether the entire identification appliance 100 is a disposable device, a disposable device attached to a reusable transponder module, or a reusable device. When tampering is detected, the circuit may disable the identification appliance 100 or disable a function or functions of identification appliance 10. Additionally, the circuit may indicate that tampering has occurred by activating a display, alarm, LED and the like, or by informing a person or another device of the tampering. Further, the identification appliance 100 may be physically securely fastened such that tampering or removal of the appliance 100 would destroy its function or render such tampering or removal evident. The securement may be permanent for the usage life of the appliance 10, or may be temporary (e.g., defeatable by an authorized procedure). In the case of temporary securement, the identification appliance 100

may be re-used and re-secured by an authorized agency or person.

Detail Description Paragraph:
[0029] When the improved identification appliance 100 enters the operative range of a local wireless communication network 10, the improved identification appliance 100 and the local wireless communication network 10 may communicate with each other. The data storage device contains the information and data for the improved identification appliance 100. For example, the data storage device may contain identification information about the authorized bearer of the improved identification appliance 100, which the identification appliance 100 can transmit to the wireless communication network 10. The identification information can include any kind of information about the authorized bearer such as his name, address, phone number, passport number, driver's license data, social security number, credit card information, fingerprint data, biometric voice characteristics, retinal characteristics and so on. This information may be written or printed visual information. For example, the identification appliance 100 may have a label or a printable surface to contain the information. The written or printed information may include data that is perceivable to humans, animals, or machines. For example, the data may be alphanumeric data, optical character recognizable data (such as bar codes), images, photographs, magnetically readable data, and/or biometric data such as fingerprint, retina, or voice data.

Detail Description Paragraph:
[0032] The connection of the improved identification appliance 100 to the wireless communication network 10 facilitates the distribution of information to and from the identification appliance 100. In other words, a wireless communication network 10 may transmit data to or receive data from an improved identification appliance 100 residing within its range. Because information may be stored electronically in the data storage device on the improved identification appliance 100, that information may be communicated to a "reader" or a wireless communication network 10 located in any site such as a hospital, prison, jailhouse, office, amusement park, concert hall and public transportation system such as an airplane, or airport.

Detail Description Paragraph:
[0037] Either a single node or multiple node approach may be used to monitor and otherwise handle a plurality of identification appliances 100. FIG. 3 is a high level representation of an example embodiment of a single node network that is adapted to interact with one or more identification appliances. A master node 140 in this example embodiment comprises a controller 142, a wireless communication circuit 144 and an interface circuit 146. Like the wireless communication circuit 122 of the identification appliance 100, the wireless communication circuit 144 of the master node 140 may enable the master node 140 to communicate with any type or types of devices, systems, or networks over any kind of wireless communication protocol, such as Bluetooth. The controller circuit 142 controls the wireless communication circuit 144 as well as other functions of the master node 140. The controller 142 may comprise, for example, a microprocessor, microcontroller, ALU, CPU, programmable gate array, control circuit, discrete analog or digital hardware and software. The wireless communication circuit 144 may receive, transmit and/or receive and transmit signals via an antenna 148. The interface circuit 146 in this example embodiment allows the master node 140 to connect to other networks such as a local area network (LAN), a wide area network (WAN), a storage area network (SAN), World Wide Web or Internet, or other public or private networks 150. The additional network 150 may be coupled to other devices such as a user's computer, a patient's personal computer 160, a medical professional's computer 162, a database server 164 and various application servers 166. The master node 140 may communicate via antenna 148 to any number N of identification appliances 100. For example, if the master node 140 is in a hospital or medical facility, the improved identification appliance 100 may be wristbands attached to patients' wrists. In this example, each patient's wristband 100 would communicate to the master node 140

through an antenna 134 embedded or otherwise coupled to the communication circuit 122 of the wristband 100. Various functions based on wireless communications may be implemented as described, for example, in this disclosure.

Detail Description Paragraph:
[0045] Vital patient data may be collected electronically by sensory devices connected to the patient's improved identification appliance 100. Various types of biometric sensors and biometric wristbands are described in another U.S. patent application filed concurrently, titled "Enhanced Identification Appliance", U.S. patent application Ser. No. ______. For example, such biometric data may include any images of or data about the wearer's fingerprints, retina, iris, or face, or a time domain or frequency domain response of the wearer's voice, or a biochemical assay of the wearer's scent, blood, or breath. In other words, the biometric data may be related to a person's signature, signature plus handwriting dynamics, iris, retina, face recognition, voiceprint, voiceprint and voice stress, fingerprint, other skin pattern, chemical signature (e.g., smell, blood, sweat), DNA signature, or some electric, magnetic, acoustic, or other biometric characteristic. Alternatively, the biometric sensor may provide data about the wearer for purposes other than for identification. For instance, the biometric sensor may be incorporated into the identification appliance to monitor or detect the wearer's pulse rate, heart electrical signals, blood pressure, insulin levels and the like, where such biometric data may be transmitted to other devices (such as monitoring computers at a hospital) constantly, intermittantly, or upon alert conditions. The patient data may be telemetered to one or more readers within the proximity of 100 meters. The wireless communication network 10 may be connected to the Internet, a local area network (LAN), or a personal computer (PC) by customary means known to those of skill in the art. Another option is to set alarm thresholds (e.g., for the patient's body temperature), which when such bounds are exceeded, the patient's improved identification appliance 100 alerts a person or device via pager, telephone, or the Internet in an email. The improved identification appliance 100 may call 911 or another emergency phone number.

Detail Description Paragraph:
[0050] Another alternative embodiment is an improved identification appliance 100 which permits a two-way voice communication between the wearer (e.g., a patient) and another person (e.g., family or medical professionals) so the wearer can make and take calls without moving to find the telephone. Instead the wearer simply puts his improved identification appliance 100 to the vicinity of his mouth. The improved identification appliance 100 has circuitry 130 to detect a voice signal by using standard speech recognition techniques well known in the art. Accordingly, the improved identification appliance 100 may have audio transducers for audio input or output, circuitry or firmware for processing speech sound and providing two-way speech communication with remote units, and circuitry or firmware for deriving biometric data from speech sound.

Detail Description Paragraph:
[0054] The improved identification appliance 100 may have other optional features. For example, if secured communications is required, communications may be encrypted. Alternatively, the unique biometric qualities of the user's voice may be transmitted, received, or processed in the improved identification appliance 100 - with a known modulation scheme.

Detail Description Paragraph:
[0059] One application in which the improved identification appliance 100 may be used is airline passenger transportation. The improved identification appliance 100 may incorporate fingerprint or hand-oriented biometric data about the authorized bearer, which information is stored in the data storage device. Such information may be provided visually on the identification appliance 100, if desired. An airline, prior to permitting a passenger to board an airplane, may use a corresponding reader kiosk to read the identification appliance 100 electronically

or optically and check the user's fingerprint when his finger is pressed on a fingerprint scanner. Optionally, the user had his fingerprint scanned earlier (e.g., during ticketing or issuance of the identification appliance) and information about that scanned fingerprint is stored in the data storage device on the identification appliance 100. Then when the user has his fingerprint scanned at the gate terminal of the airline prior to boarding the airplane, the user has his fingerprint scanned again, which scan is digitally processed and compared to the information stored in the data storage device on the identification appliance 100 regarding the earlier scanned fingerprint. Any discrepancies between the two fingerprint scans would alert the airline security personnel. The reading device may be constructed so that the fingerprint scanner and the identification appliance reader are in close proximity and isolated from electromagnetically interfering sources, as well as unauthorized surveillance. For example, a hand tunnel can be used where the tunnel both reads the identification appliance and scans the fingerprint (or handprint) at the same time. This would ensure simultaneous reading of the fingerprint and its digitized signature to deter fraud or identification appliance transference.

CLAIMS:

14. The identification appliance of claim 1 wherein the identification data includes biometric data about the authorized bearer.

15. The identification appliance of claim 14 wherein the biometric data includes fingerprint, voice, or retinal characteristics.

34. The method of claim 23 wherein the transmitting of identification data includes transmitting biometric data about the person.

35. The method of claim 34 wherein the biometric data includes fingerprint, voice, or retinal characteristics.

Previous Doc Next Doc Go to Doc#